ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution
January 10, 2008 – P.T. 2008.01

Section

20.1 Purpose

The purpose of this Administrative Procedure is to establish the Department's policy regarding the access, use, maintenance and disclosure of electronic communication, and data distribution, which includes, but is not limited to, electronic mail and Internet usage. Electronic mail or E-mail has become an essential method of communication that is accessible to all Department of Children and Family Services (DCFS) staff. The Department encourages and supports the use of E-mail to facilitate timely and efficient business-related communications; however, there are some basic principles that govern the use of electronic communication and data distribution.

- The Department's electronic mail and Internet systems should be used only for business-related communications and research.
- Department employees and other authorized users should have no expectation of privacy in anything they access, create, store, send or receive when using the Department's electronic mail and Internet systems.
- All users of the Department's electronic mail and Internet systems are required to use these resources in a responsible, professional, ethical and lawful manner.
- E-mail or Internet, used inappropriately, could result in lawsuits, costly litigation and/or employee discipline.
- The sending of E-mail does not absolve the sender from communicating orally with the recipient on critical job-related matters or tasks.
- E-mail encryption and security is solely to be provided via the CMS Public Key system implemented, no other variants are allowed.

- All department web-based or Internet accessible applications must use Secure Sockets Layer, at a minimum of 128-bit key strength, to secure the communications channel between the connecting client and the server.
    - Only department web-based applications that are not available via the Internet may use a self signed certificate.
    - All Internet available applications must use a certificate provided by a certified third party (GTE Cyber Trust, Verisign,, Entrust, etc.), and may not be a self-signed certificate.
- All department email must include the following disclaimer and statement of confidentiality.
    - "PRIVILEGED AND CONFIDENTIALITY NOTICE: This email (and/or the documents accompanying such) may contain privileged/confidential information. Such information is intended only for the use of the individual or entity above. If you are not the named or intended recipient, you are hereby notified that any disclosure, copying, distribution, or the taking of any action in reliance on the contents of such information is strictly prohibited. If you have received this transmission in error, please immediately notify the sender by telephone to arrange for the secure return of the document."

Electronic Data Distribution

- All data distribution shall be implemented or approved by the Office of Information Technology Services (OITS).
- Data distribution standards and methodologies will be observed at all times to ensure the quality and security during delivery.
- Data movement via physical devices such as flash, removable hard drives, tape, etc. shall meet with OITS approval.

VPN/Remote Access

- VPN tunnel encryption must meet a minimum of utilizing 3DES or AES encryption for the secure tunnel.
- Usage should be approved by OITS and user's business manager/supervisor.
- Usage is restricted to DCFS employee's or contracted business partners, to utilize for access to DCFS applications and services only.
- Any and all VPN connectivity constitutes an acceptance of the "acceptable use policies" of DCFS and it's information and computing systems. All VPN connections are subject to investigation, monitoring.

This Administrative Procedure should be considered an extension and further clarification of the information contained in the Department's Internet User's Guide (see Appendix B).

20.2 Definitions

CYCIS (Child and Youth Centered Information System) – confidential information of persons served by the Department of Children and Family Services is stored in the CYCIS database.

Electronic Mail System - the State's messaging system that depends on computing equipment to create, send, forward, receive, reply to, transmit, store, hold, copy, view, print, and read electronic mail.

Electronic Mail (E-mail) - any electronic computer document or message created, sent, forwarded, received, replied to, transmitted, stored, copied, downloaded, displayed, viewed, read, or printed via the Internet or Intranet.

FTP – a communications protocol governing the transfer of files from one computer to another over a network.

Internet - a group of independent, self-defined, and self-contained computer communication areas. Internet connections enable access to the Internet (a.k.a. the World Wide Web) when appropriate software has been installed on a workstation.

Intranet - a self-contained computer communication network that is strictly internal to the Department and authorized users.

MARS (Management and Accounting Report System) – confidential information of persons served the Department of Children and Family Services is stored in the MARS database.

Remote Access (RAS) – a dial up method of access to the DCFS network using modems and phone lines.

SACWIS means the (State Automated Child Welfare Information System) - Confidential information of persons served by the Illinois Department of Children and Family Services is stored in the SACWIS database.

SACWIS search function - the mechanism by which authorized SACWIS users may retrieve information maintained in the Department's database regarding child abuse and neglect investigations, child welfare service cases, and related information involving mandated reporters and Department personnel.

VPN – a virtual private network that provides a means to access the DCFS network from other networks outside of DCFS.

20.3 Permissible Uses of Electronic Mail, Internet and Data Distribution

a) Authorized Users

Only Department staff, authorized contractual staff, and private agencies using the DCFS network are considered authorized users of the Department's electronic mail, Internet systems, and other data distribution methods.

b) Purpose of Use

1) Electronic Mail and Internet

Internet usage, electronic mail, or the use of any Department resources for electronic mail should be related to Department business. This includes union-related business as stipulated in the agreements between the Department of Central Management Services and the applicable collective bargaining entities.

2) SACWIS, CYCIS, MARS, and Other Search Function

The SACWIS, CYCIS, MARS, and other search function shall be limited to use by authorized persons that have need of specific database information for the accomplishment of assigned case management functions.

20.4 Transmission of Confidential Information

Confidential information may be transmitted only as authorized under **Rules** and **Procedures 431**, **Confidentiality of Personal Information of Persons Served by the Department of Children and Family Services**. Information related to the Comprehensive Medicaid Billing System and Medicaid Community Mental Health Services shall remain confidential and may only be transmitted by authorized persons in accordance with Rules and Procedures 431, and Policy Guides 2003.04 (Comprehensive Medicaid Billing System/Medicaid Billing System) and 2003.05 (Health Insurance Portability and Accountability Act).

Additionally, any transmission of confidential information must include the statement:

> "PRIVILEGED AND CONFIDENTIALITY NOTICE: This email (and/or the documents accompanying such) may contain privileged/confidential information. Such information is intended only for the use of the individual or entity above. If you are not the named or intended recipient, you are hereby notified that any disclosure, copying, distribution, or the taking of any action in reliance on the contents of such information is strictly prohibited. If you have received this transmission in error, please immediately notify the sender by telephone to arrange for the secure return of the document."

20.5 Prohibited Uses of Electronic Mail or Internet

Displaying or disseminating materials that can be considered by some people to be obscene, racist, sexist, or otherwise offensive may constitute harassment by creating a hostile work environment. Accessing non-business related Internet sites may subject the user to discipline, up to and including discharge. Furthermore, unintended usage or unauthorized access or interference may subject the employee and/or the Department to legal action. Consequently, the Department requires appropriate standards of conduct to be employed when using electronic mail or Internet.

Specific prohibited uses of electronic mail include, but are not limited to:

- Using electronic mail systems for any purpose restricted or prohibited by State and Federal laws or regulations;
- Sending electronic mail that is considered offensive to any individual or group or accessing Internet websites for non-business purposes;
- Transmitting, via the Internet, case-related information such as, but not limited to, case notes, correspondence or documents in violation of Rules and Procedures 431. Personal information of persons served by the Department shall not be transmitted using the Internet, except as approved in writing by the Director or Chief Legal Counsel for purposes of automated E-mail reminders of juvenile court hearings and case reviews. No confidential information shall be contained in an Internet E-mail message, listed in a "chat room," or otherwise referenced in any Internet communication. Personal information of persons served by the Department may be transmitted via Outlook E-mail to other Illinois state agencies when the disclosure is in accordance with Rules and Procedures 431, and the information is sent through the DCFS Outlook E-mail system by selecting the other Illinois state agency employee's name from the Outlook Global Address List. Any other method of addressing an E-mail, including typing in the state employee's full E-mail address, may result in the E-mail being transmitted via the Internet, which is prohibited; ~~.~~
- Transmitting confidential personnel, employee discipline, or employee evaluation-related information unless necessary as part of the employee's job duties within the Department;
- Sending copies of documents in violation of copyright laws;
- Unauthorized intercepting and opening of electronic mail except as required in order for authorized employees to diagnose and correct delivery problems or to monitor usage in accordance with this Administrative Procedure, or for authorized investigations pursuant to Rule 430 or other appropriate Department purposes;
- Using electronic mail to harass or intimidate others or to interfere with the ability of others to conduct Department business;
- Accessing or attempting to access websites for non-business purposes that are sexually explicit, demeaning or exploitive of minors, women or minorities or otherwise counter to the purposes of the Department;

- Unauthorized use of an individual's E-mail account (See Appendix B) other than for monitoring or investigative purposes consistent with this Administrative Procedure or Rules 430;
- Constructing an electronic mail communication so it appears to be from someone else;
- Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization;
- Downloading and installing of unauthorized software;
- Using the E-mail or Internet system to conduct statewide mailings for notifications of births, deaths, illness, parties and social events;
- Using E-mail or Internet for other such non-business related matters; or
- Including non-business related graphics within an E-mail message.
- There is a presumption that the use of chat rooms is non-business related.
- Unauthorized use of Internet access is not limited to business hours. DCFS equipment cannot be used for non-business purposes.

20.6 Prohibited Uses of the SACWIS and Any Other Search Function

Purposes for which the SACWIS search function and any other electronic means may not be used include, but are not limited to the following:

The SACWIS search function may not be used by persons other than those authorized by the Department.

- The SACWIS search function may not be used to retrieve database information for purposes other than the accomplishment of assigned duties.
- Information obtained via a SACWIS search shall not be transmitted using the Internet or contained in an Internet E-mail message, listed in conversation in a "chat room," or otherwise referenced in any Internet communication.

20.7 Statewide Business-Related Announcements

Business-related announcements to all Department users, must be directed to the following E-mail address: ANNOUNCEMENTS. Include in the first line of the message the date that you wish the announcement to be sent.

E-mail sent to this address will be reviewed for appropriateness prior to distribution. You will be contacted, if necessary, to discuss any issues with the announcement. Allow a minimum of one business day for distribution. Emergency announcements should be marked URGENT and include in the first line an explanation of the situation creating the emergency. (Note: This will be removed prior to distribution.)

20.8 Department Monitoring, Access and Disclosure

Electronic mail created or stored on Department equipment or Internet usage constitutes a Department record and is subject to the disclosure laws of the State of Illinois. The Department reserves the right to monitor, access and disclose contents of electronic mail or internet usage without the consent of the originator or the recipient of the correspondence.

The SACWIS search and the information developed from the search that is stored on Department equipment constitutes a Department record and is subject to the disclosure laws of the State of Illinois. The Department reserves the right to monitor, access and disclose contents of searches without the consent of the originator of the search.

20.9 Security

Users are advised that electronic mail messages that are transmitted, received, or stored on the Department's electronic mail systems are the property of the Department, and as such, may be considered public records. All Internet sites accessed and attempts to access are subject to monitoring by the Department. The SACWIS search and the information developed from the search that is stored on the Department's electronic systems are the property of the Department, and as such, may also be considered public records.

All Department electronic mail and Internet usage that connects to the Internet, Outlook, or AS400 systems passes through the Department of Central Management Services' (CMS) computer network. Both CMS and DCFS conduct regular back-ups of their electronic mail files. Even though the sender and recipient have discarded or deleted their copies of an electronic mail record, there may be back-up copies, either at DCFS or CMS that can be retrieved as the result of discovery requests in the course of litigation or other official inquiry.

20.10 Maintenance of Electronic Mail

All electronic records will be maintained according to the rules and timeframes set forth by the State Records Commission and the Department. Staff should preserve essential electronic business records through archiving documents on their workstation or through conventional filing and maintenance.

The Department will maintain a back-up copy of deleted E-mail transactions for 30 days, at which time they will be removed from the system. A back-up copy of the E-mail journal will be taken every 30 days of all E-mail transactions occurring in that 30-day period and will be retained for five years.

20.11 Policy Enforcement

Violations of Department E-mail or data distribution polices will subject employees to disciplinary action up to and including discharge.

20.12 Policy Acknowledgement

Users of the Department's electronic mail system and/or SACWIS search function *must* sign a **CFS 123** (**Electronic Communication and Distribution Certificate of Understanding**) acknowledging that they have read and understand the conditions and terms of this agreement (See Appendix A). The signed copy is to be maintained in the employee's on-site personnel file and a copy sent to the Office of Employee Services for inclusion in the employee's personnel file. Failure to sign a CFS 123 will result in loss of network privileges.

ADMINISTRATIVE PROCEDURE #20
Electronic Communication and Distribution Certificate of Understanding
January 10, 2008 – P.T. 2008.01

APPENDIX A

CFS 123
Rev 1/2008

State of Illinois
Department of Children and Family Services

ELECTRONIC MAIL COMMUNICATION AND DISTRIBUTION CERTIFICATE OF UNDERSTANDING

1) I acknowledge that I have read Administrative Procedure #20, Electronic Communication and Distribution, and that I am responsible for abiding by the policies contained, therein.

2) I understand that the use of computer equipment, software and the electronic mail system is for State of Illinois business only.

3) I understand that unauthorized transmittal of confidential information via the electronic mail system is prohibited.

4) I understand that only non-confidential information may be transmitted across the Internet (outside the Department's Outlook E-mail system) and that I may never use specific names of wards (except as approved in writing by the Director or Chief Legal Counsel for purposes of automated E-mail reminders of juvenile court hearings and case reviews), perpetrators, witnesses, or any other persons served by the Department in an Internet E-mail message, listed in conversation in a "chat room," or otherwise referenced in any Internet communication.

5) I understand that information obtained via a SACWIS search shall not be transmitted using the Internet or contained in an Internet E-mail message, listed in conversation in a "chat room," or otherwise referenced in any Internet communication.

6) I understand that electronic mail records are considered Department business records subject to Federal and State freedom of information laws and official State of Illinois record retention rules.

7) I understand there is no expectation of privacy in any E-mail, Internet or SACWIS search document I create, store, send, or receive when using the Department's electronic mail and Internet systems.

8) I understand that a violation of this policy may result in disciplinary action, up to and including possible discharge, as well as civil and criminal liability that my action may create.

Signature: _____ Date: _____

Printed Name: _____

Work Location: _____

This page intentionally left blank.

APPENDIX B
INTERNET USER'S GUIDE

Purpose

The purpose of this user's guide is to supply general information necessary to access and use the Internet and World Wide Web provided by the State of Illinois and the Department of Children and Family Services.

Background

The Internet is a group of independent, self-defined, and self-contained computer communication areas. Internet connections enable access to the World Wide Web when appropriate software has been installed on the PC. Available services and functions can be grouped into home pages, E-mail messages, chat rooms, and search requests. Access is supplied to authorized state workers and state service providers through individual state agencies and CMS.

Internet Connection

Accessing the Internet and World Wide Web through State of Illinois DCFS facilities is restricted to state employees and individuals working under a current contract to provide a state service. Access is granted by DCFS Information Services Division (ISD) only when justification is provided to ISD, authorization is obtained from DCFS management, and the Information Technology Certificate of Understanding is signed. Internet use requires a PC with at least a 386 processor (486 is preferred), 8 meg of RAM, 12 meg of hard disk space, and a modem operating at no less than 14.4 kbs.

Responsibilities

Regardless of the Internet Service Provider (ISP) used, device type (desktop or portable computer), or connection location (office or home), State employees are expected to follow prudent security and confidentiality guidelines defined here and in other DCFS, CMS, and State rules, policies, procedures, and guidelines. If you have any questions on security, Internet access or use, or other technical questions, please contact the ISD Help Desk at 1-877-800-3393. If you have any questions regarding confidentiality, please contact your supervisor.

Security & Confidentiality

Use of any DCFS computer, software, data, or communication access service is strictly limited to State of Illinois business.

No intentional access, display, or creation of offensive, malicious, illegal, or non-business related material is permitted.

Each individual is responsible for ensuring that Department expectations, policies, procedures and guidelines are followed.

Confidential data, as defined in Department **Rule** and **Procedure 431**, is prohibited from being transmitted using the Internet. No confidential information shall be contained in an

Internet E-mail message, listed in conversation in a "chat room", or otherwise referenced in any Internet communication.

The Department reserves the right to cancel any Internet account without notice which it deems in violation of Department or state policy or policy intent.

In order to ensure that the Internet is used in accordance with Department policies, ISD reserves the right to monitor usage, connections, and content of Internet communications.

Any damage caused by introduction of a computer virus via unauthorized use of unprotected software may result in financial restitution against the individual who introduced the virus. Contact ISD for virus protection and eradication software.

Disciplinary action up to and including discharge may result if these policies are not followed.

Getting Started

Employees must document justification for Internet services and obtain approval from their Deputy Director. A request including both justification and approval must then be submitted to the ISD Manager.

The requesting office is responsible for the cost of acquiring an additional phone line, if one is necessary. The requesting office may also be responsible for the cost of any additional hardware required.

Before Internet access is granted, a user must sign an "Information Technology Certificate of Understanding". This certificate lists the limitations regarding types of information that can be transmitted using data communication devices and reiterates confidentiality concerns. The signed copy is to be maintained in the employee's on-site personnel file and a copy sent to the Office of Employee Services for inclusion in the employee's personnel file.

Once ISD grants Internet access, ISD will contact CMS for issuance of a login id and password and an E-Mail id and password. ISD will install the necessary software and will provide training on using the Internet. If additional problems are encountered after training, contact the ISD Help Desk for assistance.

Usage

The Internet may be used for DCFS business only. This includes, but is not limited to, child welfare research, E-mailing out-of-state child welfare officials and professionals, etc. Use of confidential information is prohibited on the Internet. Personal usage involving private business-related matters, communications with non-departmental acquaintances, creating or forwarding of "chain" letters, games, gambling, non-business related chat rooms, sports information or the like is also prohibited. Users may not download software, including any on-line services, from an Internet site, regardless of whether it is fee-based or without charge, unless authorized by the ISD manager. To prevent unauthorized access to State networks and data, users must not have an active connection (be logged on) to either the AS/400 or the host system (PROFS or IMS)

concurrently with an Internet connection on the same machine, either at the office or at home.

Notify the ISD Help Desk IMMEDIATELY of any unexplained, strange occurrences regarding your account. It is possible for an account to be infected with a virus, "hacked" or otherwise compromised. Once an account has been compromised, it places the entire system at risk. Internet sessions are terminated if no activity has occurred for 5 minutes or if contiguous connect time exceeds 4 hours.

This page intentionally left blank.

AP #20 ELECTRONIC MAIL
July 3, 2000 – P.T. 2000.12

INFORMATION TECHNOLOGY CERTIFICATE OF UNDERSTANDING

I, _____, do hereby agree to abide by all rules, policies, and
(please print)
procedures of the Department of Children and Family Services, the Department of Central Management Services, and the State of Illinois regarding information technology activities.

Specifically, I agree to:

1. Use computer equipment, computer software, PROFS, the Internet, and any other data processing device, software, application, or service for State of Illinois business only.

2. Transmit only non-confidential information across the Internet or other data communication service and never to use specific names of wards, perpetrators, or witnesses in any conversation on the Internet.

3. Restrict Internet access to only those areas directly related to State of Illinois business and to refrain from accessing, displaying, or creating any offensive, malicious, or illegal material.

4. Accept that Internet E-mail is considered Department business records subject to Federal and State freedom of information laws and official State of Illinois record retention rules.

5. Acknowledge that, because DCFS will be monitoring my Internet usage, I do not expect privacy in my Internet E-mail communications.

6. Accept that any violation of DCFS or CMS Internet usage policy may result in disciplinary action up to and including discharge.

7. Acknowledge that downloading from or uploading to the Internet copyrighted material that will then be distributed to other individuals is prohibited.

_____ _____
(SIGNATURE) **(DATE)**

_____ _____
(WORK LOCATION) **(WORK PHONE)**

This page intentionally left blank.